What Is Claimed Is:

1. A data generating apparatus comprising:

a data-for-main-checking memory unit for holding first data;

a data-for-secondary-checking memory unit for holding second data;

an encrypting key generation unit for generating an encrypting key from data stored in the data-for-secondary-checking memory unit; and

an encryptor for encrypting data stored in the data-for-main-checking memory unit with the encrypting key generated by the encrypting key generation unit, wherein

data that includes at least one of the result of encrypting by the encryptor and the data stored in the data-for-secondary-checking memory unit is generated.

2. A data generating apparatus according to Claim 1, further comprising:

a previous key memory unit for holding a previous key, wherein the encrypting key generation unit also uses the previous key stored in the previous key memory unit in generating an encrypting key.

3. A data generating apparatus according to Claim 1, wherein the data stored in the data-for-main-checking memory unit is a result of decrypting prescribed encrypted data.

4. A data generating apparatus according to Claim 1, wherein the data stored in the data-for-main-checking memory

unit is a signature for prescribed data.

5. A data generating apparatus according to Claim 1, wherein the encrypting key generation unit is composed of a one-way function, and a result of inputting the data stored in the data-for-secondary-checking memory unit into the one-way function is the encrypting key.

6. A data generating apparatus according to Claim 2, further comprising:

a previous key encrypting key memory unit for holding a previous key encrypting key for encrypting the previous key; and

a previous key encryptor for encrypting the previous key with the previous key encrypting key stored in the previous key encrypting key memory unit.

7. A data generating apparatus according to Claim 1, wherein the encrypting performed by the encryptor is symmetric key encrypting.

8. A data generating apparatus according to Claim 1, wherein the encrypting performed by the encryptor is multiplication or division using the data stored in the data-for-main-checking memory unit and the encrypting key generated by the encrypting key generation unit under a prescribed modulus number.

9. A data generating method comprising the steps of:

generating an encrypting key from first data;

encrypting second data, capable of being checked whether it includes a prescribed characteristic, with the encrypting

key; and

generating data including at least one of the first data and the encrypted second data.

10. A data verifying apparatus comprising:

a data-for-main-checking memory unit for holding first data;

a data-for-secondary-checking memory unit for holding second data;

a decrypting key generation unit for generating a decrypting key from data stored in the data-for-secondary-checking memory unit;

a decryptor for decrypting data stored in the data-for-main-checking memory unit with the decrypting key generated by the decrypting key generation unit; and

a check unit for checking whether the data decrypted by the decryptor has a prescribed characteristic.

11. A data verifying apparatus according to Claim 10, further comprising:

a previous key memory unit for holding a previous key, wherein the decrypting key generation unit, in generating a decrypting key, also uses the previous key stored in the previous key memory unit.

12. A data verifying apparatus according to Claim 10, wherein the check unit checks whether the data decrypted by the decryptor is a result of decrypting prescribed data with a prescribed decrypting key.

13. A data verifying apparatus according to Claim 10,

wherein the check unit checks whether the data decrypted by the decryptor is a signature signed with a prescribed signature key.

14. A data verifying apparatus according to Claim 10, wherein the decrypting key generation unit is composed of an one-way function, and a result of inputting the data stored in the data-for-secondary-checking memory unit into the one-way function is the decrypting key.

15. A data verifying apparatus according to Claim 10, further comprising:

a previous key memory unit for storing an encrypted previous key;

a previous key decrypting key memory unit for storing a decrypting key for decrypting the encrypted previous key; and

a previous key decryptor for decrypting the encrypted previous key stored in the previous key memory unit with the decrypting key stored in the previous key decrypting key memory unit.

16. A data verifying apparatus according to Claim 10, wherein the decrypting performed by the decryptor is decrypting in symmetric key algorithm.

17. A data verifying apparatus according to Claim 10, wherein the decrypting performed by the decryptor is multiplication or division using the data stored in the data-for-main-checking memory unit and the decrypting key generated by the decrypting key generation unit under a prescribed modulus number.

18. A data verifying method comprising the steps of:

generating a decrypting key from first data;

decrypting second data with the decrypting key; and

checking whether a result of decrypting includes a prescribed characteristic.

19. A data processing apparatus comprising a data generating apparatus and a data verifying apparatus for verifying the integrity of data generated by the generating apparatus, wherein:

the data verifying apparatus further comprises:

a reference value memory unit for holding first data;

a first data-for-secondary-checking memory unit for holding second data;

a decrypting key generation unit for generating a decrypting key from data stored in the first data-for-secondary-checking memory unit;

a decryptor for decrypting the data sent from the data generating apparatus with the decrypting key generated by the decrypting key generation unit; and

a verification unit for checking whether the data decrypted by the decryptor has a prescribed relationship with the first data stored in the reference value memory unit, and

the data generating apparatus further comprises:

a data-for-main-checking generation unit for generating third data from the first data sent from the data verifying apparatus;

a data-for-secondary-checking memory unit for holding fourth data;

an encrypting key generation unit for generating an encrypting key from the data stored in the second data-for-secondary-checking memory unit; and

an encryptor for encrypting the third data generated by the data-for-main-checking generation unit with the encrypting key generated by the encrypting key generation unit, wherein

the data verifying apparatus sends the first data stored in the reference value memory unit to the data generating apparatus;

the data generating apparatus generates the third data from the first data sent from the data verifying apparatus by the data-for-main-checking generation unit, generates data by encrypting the third data by the encryptor, and further sends the generated data to the data verifying apparatus; and

the data verifying apparatus decrypts with the decryptor the data sent from the data generating apparatus, and checks with the verification unit whetehr a result of decrypting has a prescribed relationship with the first data stored in the reference value memory unit.

20. A data processing apparatus according to Claim 19, wherein the third data generated by the data generating apparatus is a result of decrypting with a prescribed decrypting key the first data sent from the data verifying apparatus, and the verification unit of the data verifying apparatus checks whether the result of decrypting of data sent from the data generating apparatus is a result of decrypting the first data.

21. A data processing apparatus according to Claim 19,

wherein the third data generated by the data generating apparatus is a signature generated by signing the first data sent from the data verifying apparatus with a prescribed signature key, and the verification unit of the data verifying apparatus checks if a result of decrypting the data sent from the data generating apparatus is a correct signature with respect to the first data.

22. A data processing apparatus according to Claim 19, wherein

the data generating apparatus further comprises:

a commitment random number memory unit for holding a random number; and

a commitment generation unit for generating a commitment from the random number stored in the commitment random number memory unit, and

the data verifying apparatus further comprises:

a commitment memory unit for storing the commitment sent from the data generating apparatus, and wherein

the data generating apparatus sends, before it receives the first data from the data verifying apparatus, the commitment generated by the commitment generation unit to the data verifying apparatus,

the data-for-main-checking generation unit, also uses a random number stored in the commitment random number memory unit for generating the third data to be verified, and

the data verifying apparatus, when its check unit performs checking, also uses the commitment stored in the commitment memory unit.

23. A data processing apparatus according to Claim 19, wherein the decrypting key generation unit of the data verifying apparatus is composed of an one-way function, a result of entering the data stored in the first data-for-secondary-checking memory unit into the one-way function is the decrypting key, the encrypting key generation unit of the data generating apparatus is composed of the same one-way function as that of the decrypting key generation unit of the data verifying apparatus, and a result of entering the data stored in the second data-for-secondary-checking memory unit into the one-way function is the encrypting key.

24. A data processing apparatus according to Claim 19, wherein the data verfying apparatus further comprises:

a first previous key memory unit for holding a previous key, and

the decrypting key generation unit, when it is to generate the decrypting key, also uses the previous key stored in the first previous key memory unit, and

the data generating apparatus further comprises:

a second previous key memory unit for holding the previous key, and

the encrypting key generation unit, when it is to generate the encrypting key, also uses the previous key stored in the second previous key memory unit.

25. A data processing apparatus according to Claim 24, wherein:

the data generating apparatus further comprises:

a previous key encrypting key memory unit for storing a previous key encrypting key for encrypting the previous key; and

a previous key encryptor for encrypting the previous key with an encrypting key stored in the previous key encrypting key memory unit, and

the data verifying apparatus further comprises:

a previous key decrypting key memory unit for storing a previous key decrypting key for decrypting the encrypted previous key; and

a previous key decryptor for decrypting the encrypted previous key with a previous key decrypting key stored in the previous key decrypting key memory unit, wherein

the data generating apparatus encrypts the previous key stored in the second previous key memory unit with the previous key encryptor using the encrypting key stored in the previous key encrypting key memory unit, and sends the result to the data verifying apparatus, and

the data verifying apparatus decrypts the encrypted previous key sent from the data generating apparatus with the previous key decryptor using the decrypting key stored in the previous key decrypting key memory unit, and stores the result in the first previous key memory unit.

26. A data processing apparatus according to Claim 19, wherein

the data verifying apparatus sends data held in the first data-for-secondary-checking memory unit to the data generating

apparatus, and

the data generating apparatus stores the data sent from the data verifying apparatus in the second data-for-secondary-checking memory unit for use in generation of the encrypting key.

27. A data processing apparatus according to Claim 19, wherein

the data generating apparatus sends the data held in the second data-for-secondary-checking memory unit to the data verifying apparatus, and the data verifying apparatus stores the data sent from the data generating apparatus in the first data-for-secondary-checking memory unit for use in generation of the decrypting key.

28. A data processing apparatus according to Claim 19, wherein the encrypting performed by the encryptor is the encrypting using a symmetric key algorithm with the encrypting key, and the decrypting performed by the decryptor is the decrypting using a symmetric key algorithm with the decrypting key.

29. A data processing apparatus according to Claim 19, wherein the encrypting performed by the encryptor is multiplication or division using the third data and the encrypting key under a prescribed modulus number, and the decrypting performed by the decryptor is multiplication or division using the data sent from the data generating apparatus by the decrypting key under the same modulus number used in the encryptor.

30. A data processing apparatus comprising:

a first device comprising a first data memory means and an encrypting means; and

a second device comprising a second data memory means, a decrypting means and a verifying means, wherein

the first device encrypts prescribed data to be verified with the encrypting means on the basis of data stored in the first data memory means, and the second device decrypts the encrypted prescribed data to be verified with the decrypting means on the basis of data stored in the second data memory means, verifies the integrity of the result of decrypting with the verifying means, and, if the data is successfully verified, authenticates the identity between the data stored in the first data memory means and the data stored in the second data memory means.

31. A data processing apparatus according to Claim 30, wherein at least part of the data stored in the first data memory means is data sent from the second device.

32. A data processing apparatus according to Claim 30, wherein at least part of the data stored in the second data memory means is data sent from the first device.